

13th ICCRTS
“C2 for Complex Endeavors”

**C2 for Computer Networked Operations: Using Computational
Experimentation to Identify Effects on Performance in Organizational
Configurations within the Larger Network-Centric Environment**

Organizational Issues Track¹

*****Student Paper*****

Major Jack L. Koons III, Lieutenant JG Nikolaos Bekatoros HN,
Dr. Mark E. Nissen

Point of Contact: Major Jack Koons
Naval Postgraduate School
School of Operational and Information Sciences
589 Dyer Road, Monterey, CA 93943-5000
831-656-1006
jlkoons@nps.edu

Abstract

The role of computer networked operations (CNO) has taken on greater importance with the rise of network-centric warfare. Comprised primarily of defense, attack, and exploitation, the technological capabilities are growing exponentially, as is the rate of data exchange, yet the organizational configurations supporting CNO are slow to anticipate and react. This presents a serious issue in terms of command and control (C2), as such organizations do not fit well with their highly dynamic environments, nor are they suited well to the missions and expectations placed upon them. Contingency Theory offers excellent potential to inform leaders and policy makers regarding how to bring their C2 organizations and approaches into better fit, and hence to improve CNO performance. The key research question is, which organizational configurations provide the best CNO performance within the network-centric environment? Building upon a half century of rich, theoretical and empirical research in Contingency Theory, we construct computational models of CNO set within different organizational configurations taken from both theory and practice, and we employ the method of computational experimentation to examine the comparative performance of such different configurations. Results elucidate important insights into CNO C2, suitable for immediate policy and operational implementation, and expand the growing empirical basis to guide continued research along these lines.

¹ This research is sponsored in part by the Office of the Assistant Secretary of Defense for Networks and Information Integration, through its Command & Control Research Program and the Center for Edge Power at the Naval Postgraduate School.

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE JUN 2008		2. REPORT TYPE		3. DATES COVERED 00-00-2008 to 00-00-2008	
4. TITLE AND SUBTITLE C2 for Computer Networked Operations: Using Computational Experimentation to Identify Effects on Performance in Organizational Configurations within the Larger Network-Centric Environment				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School,School of Operational and Information Sciences,589 Dyer Road,Monterey,CA,93943				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES 13th International Command and Control Research and Technology Symposia (ICCRTS 2008), 17-19 Jun 2008, Seattle, WA					
14. ABSTRACT The role of computer networked operations (CNO) has taken on greater importance with the rise of network-centric warfare. Comprised primarily of defense, attack, and exploitation, the technological capabilities are growing exponentially, as is the rate of data exchange, yet the organizational configurations supporting CNO are slow to anticipate and react. This presents a serious issue in terms of command and control (C2), as such organizations do not fit well with their highly dynamic environments, nor are they suited well to the missions and expectations placed upon them. Contingency Theory offers excellent potential to inform leaders and policy makers regarding how to bring their C2 organizations and approaches into better fit, and hence to improve CNO performance. The key research question is, which organizational configurations provide the best CNO performance within the network-centric environment? Building upon a half century of rich, theoretical and empirical research in Contingency Theory, we construct computational models of CNO set within different organizational configurations taken from both theory and practice, and we employ the method of computational experimentation to examine the comparative performance of such different configurations. Results elucidate important insights into CNO C2, suitable for immediate policy and operational implementation, and expand the growing empirical basis to guide continued research along these lines.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 35	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Introduction

The role of computer networked operations (CNO) has taken on greater importance with the rise of network-centric warfare in our offensive capabilities and defensive responsibilities (CRS Report to Congress, 2007; Whitehouse, 1998). Comprised primarily of defense, attack, and exploitation, CNO technological capabilities are growing exponentially (United States Army Training and Doctrine Command, 2005), as is the rate of data exchange, yet the organizational configurations supporting CNO are slow to anticipate and react (Bryan, 2003). This presents a serious issue in terms of command and control (C2), as such organizations do not fit well with their highly dynamic environments, nor are they suited well to the missions and expectations placed upon them. Indeed, the Department of Defense (DoD) is grappling with decisions concerning the effective organizational structure to conduct CNO. These decisions demand a firm grasp of the operational requirements as well as an understanding of the CNO mission and organizational design issues. Contingency Theory offers excellent potential to inform leaders and policy makers regarding how to bring their C2 organizations and approaches into better fit, and hence to improve CNO performance. The key research question is, which organizational configurations provide the best CNO performance within the network-centric environment?

Drawing from Gateau et al. (2007), we understand how recent advances in computational organization theory (e.g., see Burton et al. 2002, Carley and Lin 1997, Levitt et al. 1999, Lomi & Larsen, 2001) and computational social science (see NAACSOS 2007) offer promising potential to address this question. For instance, to represent and reason about organizational processes, one can conduct computational experiments with levels of rigor and control comparable to laboratory experimentation. This can support greater internal validity and reliability than is obtainable often through fieldwork. As another instance, computational experiments can be conducted to examine myriad different organizational designs, including cases that have yet to be implemented in physical organizations (Nissen, 2005b). Moreover, mission-environmental contexts are not manipulated easily in the field, and laboratory experiments are limited generally to micro-level organizational phenomena.

The present paper represents part five in our campaign of experimentation, which began with a paper presented at the 2004 CCRTS conference (Nissen and Buettner, 2004). In that paper, the relative advantages and disadvantages of computational experimentation were presented, and this computational research method was described in terms of a complementary, empirical approach. The 2005 ICCRTS paper followed (Nissen, 2005a); it compared and analyzed more than 25 diverse organizational forms, including the Edge organization, which was shown to be theoretically distinct and uniquely differentiated from other organization forms described by prior investigators. This 2005 paper also offered a theoretical discussion and set of hypotheses about the performance of Edge and Hierarchy organization forms under different mission-environmental conditions, and provided insight into relative characteristics and behaviors of Hierarchy and Edge organizations. Then in our 2006 ICCRTS paper

(Orr and Nissen, 2006), we expanded the study to specify and model four other, classic, theoretically grounded organization forms: Simple Structure, Professional Bureaucracy, Divisionalized Form, and Adhocracy (Mintzberg, 1979, 1980). We also employed computational experimentation to compare and contrast empirically the relative performance of Hierarchy and Edge organizational forms, using a multidimensional set of performance measures, under the mission-environmental conditions at two different points in history: the Industrial Era (e.g., characterizing Cold War era missions and environments), and the 21st Century (e.g., characterizing Global War on Terror missions and environments). Finally, in our 2007 ICCRTS paper (Gateau et al., 2007), we articulated an organizational design space for the first time, discussing the model, experimental setup and results in considerable detail, as well as offering theoretical implications for the organization scholar and actionable guidance for the C2 practitioner.

Building upon a half century of rich, theoretical and empirical research in Contingency Theory—in addition to the campaign outlined above—we construct computational models of CNO set within different organizational configurations taken from both theory and practice. This enables us to articulate—very clearly through semi-formal organizational models—the kinds of organizations, work processes, technologies and people associated with CNO today. Using such models, we employ the method of computational experimentation to examine the comparative performance of different CNO organizational configurations in the mission-environmental context of CNO today and tomorrow. The following section presents a representative discussion of CNO today, along with key concepts from theory. Then we describe our computational model, present the results of computational experimentation, and draw final conclusions.

Background

We begin with an introduction to computer network operations based on current DOD doctrinal definitions. The idea is to present a representative discussion of CNO today. We then follow by summarizing briefly the central premise of Contingency Theory and outlining a set of theoretical, archetypal organization forms.

Computer Network Operations²

By US doctrine (e.g., Joint Chiefs of Staff, 2006), CNO can be viewed best as a subcomponent of information operations, which include five capabilities: psychological operations, military deception, operational security, electronic warfare and CNO (Wilson, 2007). Additionally, CNO can be subdivided further into three core components: computer network attack, defense, and exploitation. The purpose of CNO is to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure and/or enable such activities. The electronic information and infrastructure of interconnected computer systems are commonly referred to as networks, which are usually part of or connected to a larger infrastructure known as the global information grid (GIG). The GIG is the

² We appreciate the assistance with this section from Carlos Vega, both through his thesis work (Vega, 2004) and personal communications (December 2007).

globally interconnected, end-to-end set of information capabilities and associated processes. This includes the human element that enables and orchestrates myriad activities associated with information handling and processing. CNO's operating space can encompass any part of the GIG's end-to-end reach.

CNO missions are generally multifaceted, and can simultaneously include components of attack, defense and exploitation. The operations can be generally classified as offensive and defensive in nature. Offensive operations imply attacking and exploiting the adversaries' systems, and protecting (defending) the access point or point of intrusion to an adversary's network, while not compromising one's own network or techniques for intrusion. Defensive operations imply protecting one's own network from an adversary's attack and exploitation attempts. The defense of a network may include active attempts to attack and exploit one's own network to identify weaknesses and vulnerabilities. Such active attempts by authorized personnel to attack and exploit a friendly network is known as "penetration testing," not attack or exploitation, although the methods and techniques may be similar.

The present state of CNO and how to organize to manage this capability effectively is the subject of much debate currently in the executive branch of government (CRS Report to Congress, 2007). While the capabilities are being developed, the organizational structure is lagging behind. The United States armed forces are organized based on physical places called domains. Different services have primary responsibility for each domain: currently the Air Force has primary responsibility for the air and space domain; the Navy has the sea; and the Army has the land. Clearly, with increasing joint (and coalition) operations, various services (and nations) must work together across domains. With the advent of the GIG, the US armed forces are considering the extent to which cyber should be viewed as a domain (e.g., like air, space, sea or land), or a method or weapon (e.g., like airplanes, satellites, ships and tanks) to achieve objectives (Bryan, 2003; Department of Defense, 2003; Franz et al., 2007).

Consider, for instance, how Cyberspace has minimal physical presence, and hence can be viewed as a domain separate from its physical counterparts (e.g., air and space). Battles were fought only on land and then at sea for millennia, but the advent of air warfare in the 20th Century—and space operations in the 21st Century—called for new and distinct service responsibilities. New cyber responsibilities associated with CNO may call similarly for distinct service responsibilities. As another instance, CNO can be compared to the longbow weapon prior to the battle of Crécy in 1346. The longbow, a two-centuries-old weapon, proved decisive for the English in battle against larger French forces, because it was employed via different tactics. Different tactics associated with using decades-old networks as weapons may call similarly for decisive use in battle (Vega, 2004).

Theoretical Concepts

To begin, Leweling and Nissen (2007) explain how, for more than a half century, Contingency Theory has retained a central place in organization studies research. Beginning with seminal works by Burns and Stalker (1961), Woodward

(1965), Lawrence and Lorsch (1967) and others, organization theory has been guided by the understanding that no single approach to organizing is best in all circumstances. Moreover, myriad empirical studies (e.g., Woodward, 1965; cf. Mohr, 1971; Pennings, 1975) have confirmed and reconfirmed that poor organizational fit degrades performance, and many diverse organizational forms (e.g., Bureaucracy, see Mintzberg 1980; M-Form, see Donaldson, 2001; Clan, see Ouchi, 1981; Network, see Miles & Snow, 1978; Platform, see Ciborra, 1996; Virtual, see Davidow & Malone, 1992) and configurations (e.g., Machine Bureaucracy, Simple Structure, Professional Bureaucracy, Divisionalized Form, Adhocracy, see Mintzberg, 1979) have been theorized to enhance fit across an array of contingency factors (e.g., age, environment, size, strategy, technology).

The concept *organizational fit* describes how well a particular organizational form is suited to perform effectively (i.e., fit well) in a particular contingency context. For instance, *organizational technology and organizational environment* have been studied extensively as powerful contingency factors (e.g., Burns & Stalker, 1961; Harvey, 1968; Galbraith, 1973), with alternate technological and environmental characteristics (e.g., *comprehensibility, predictability, complexity, stability*) related contingently with different organizational forms (e.g., *craft, engineering*, see Perrow, 1970). Indeed, organization scholars have come to understand well how various organizational forms should and do vary to fit diverse environmental contexts. This provides the backdrop for our analysis of CNO: we seek to identify the organizational form suited best for effective performance.

Additionally, Orr and Nissen (2006) explain how a small set of theoretical, archetypal organization forms offer promise in terms of informing experimentation in the context of contingency fit. Following this line of work, we build upon Mintzberg's (1980) five, archetypal organizational configurations: Simple Structure, Machine Bureaucracy, Professional Bureaucracy, Divisionalized Form, and Adhocracy. The different configurations vary according to the structuring and predominance of their organizational parts, coordination mechanisms, design parameters, and contingency factors. Further, they are broadly applicable, mutually distinct, and derived from both theory and practice. Hence they are representative of many contemporary organizations observable in practice today, and many of the emerging organizational forms (e.g., strategic alliances, networked firms, Edge organizations) can be analyzed as hybrids through consideration of their separate parts, mechanisms, parameters and factors.

Moreover, we include the Edge organization (Alberts and Hayes, 2003) as a sixth archetype with particular applicability in the C2 domain (see Nissen, 2005a, Orr and Nissen, 2006). The Edge shares similarities with the Adhocracy (e.g., coordination by mutual adjustment, small unit size, many liaison links throughout, selective decentralization), Professional Bureaucracy (e.g., low vertical specialization, high training and indoctrination, market and functional grouping), and Simple Structure (e.g., low horizontal specialization, low formalization), but it also demonstrates several key differences, and does not correspond cleanly with any single archetype (e.g., it is characterized as an hybrid *Professional Adhocracy*—a combination of archetypes). Key to Edge

characterization is decentralization, empowerment, shared awareness and freely flowing knowledge required to push power for informed decision making and competent action to the “edges” of organizations (Alberts and Hayes, 2003), where they interact directly with their environments and other players in the corresponding organizational field (Scott, 2001). In contrast, the Edge organization shares almost no similarities with the Machine Bureaucracy (cf. high training and indoctrination), the latter to which we refer interchangeably as “Hierarchy.” Together, these six archetypes from theory inform our experimentation on CNO.

Research Design

In this section we focus on Computer Network Defense (CND), and describe a grounded model of CND as it is organized and managed today, to guide our computational model building. Defense represents a very practical point to being an investigation such as this: there is little opportunity to conduct computer attacks and exploitations if one’s own defenses are weak, and one’s own network is vulnerable. We then represent this grounded model using an agent-based modeling environment, and we formulate a second computational model to reflect an alternate approach to CND. Subsequently, we describe our experiment design to examine the comparative performance of different organizational forms.

Grounded CND Model

To understand computer network defense as it exists in the field, we canvassed the latest “best practices” gleaned from various online references as well as subject matter experts at a major Department of Defense educational institution. This immersive online and field research effort allowed us to sample from a wide range of computer network organizational approaches (educational, governmental, and corporate business). We then used the information gleaned to arrive at a general model. This model served as the framework for our agent-based modeling simulations.

The model below represents a representative computer network defense approach (e.g., organizational structure, task structure, personnel staffing, technological infrastructure), which is generalized along lines similar to those found in college campuses and like, mid-to-large-scale enterprises. Specifically, we based our organization structure and workflow process on a template used by the University of California at San Francisco Medical Center. This model was then subjected to face validation by various Department of Defense computer science instructors.

A key and recurring emphasis of CND involves responding to hacker attacks. There are various methods of categorizing a hacker attack. They typically center on one of three main profiles: 1) unauthorized activity on the host system; 2) unauthorized attempt to gain access to the host system; and 3) anomalies on the host system discovered after the fact (UCSF Medical Center, 2008). Our workflow process addresses active attempts to gain access to the host network.

Building upon our discussion above, we use the POW-ER (Projects, Organizations, and Work for Edge Research) computational modeling environment (e.g., see Gateau et al., 2007) to represent and emulate the structure and behavior of current CNO. Focusing on our purpose to test the current CNO structure with a decentralized, edge-like structure, we examine a specific CND incident: hacker attack. This approach sets common conditions to both organizational structures, providing opportunities to examine the behaviors of organizational actors performing tasks, and enabling us to represent only the most important aspects of the external environment (Simon, 1996).

In developing this model, we ground our computer representation in current practice as well as doctrine (see *Figure 1* below). As above, the CND organization and task structures for a hacker attack are based on the UCSF Medical Center, and are cross-validated by the current CND structure of a major DoD educational institution. This provides considerable external validity to our models, yet the representations remain at a relatively high level, and hence retain considerable generalizability also. The tasks required to address a hacker/penetration follow:

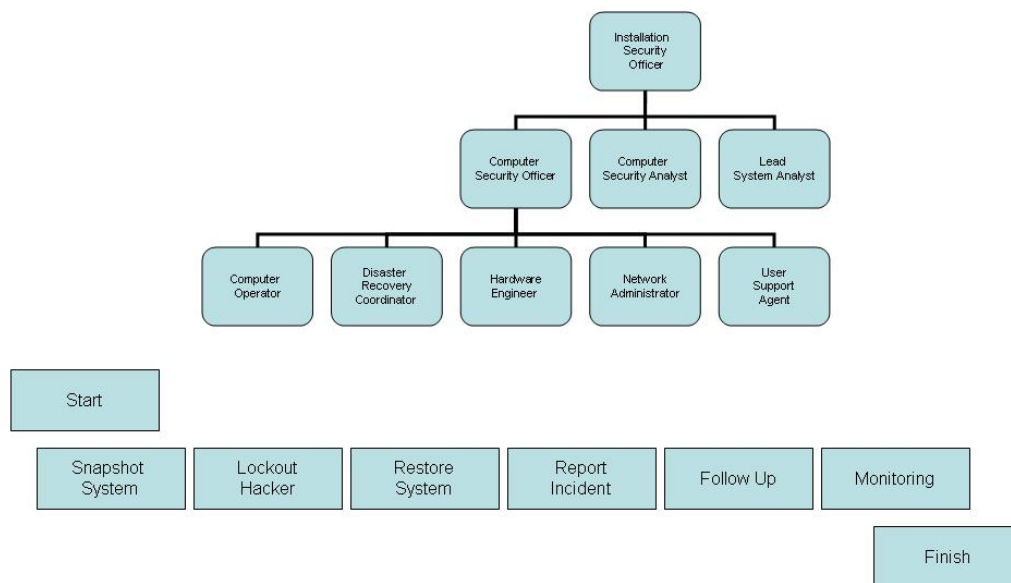


Figure 1 Computer Network Operations Organization Diagram

a) **Snapshot the System:** Make copies of all audit trail information such as system log files, the root history files, and like tasks, and get a listing of all active network connections.

b) **Lockout the Hacker:** Kill all active processes for the hacker/cracker, and remove any files or programs that may have been left on the system. Change passwords for any accounts that were accessed by the hacker/cracker.

c) **Restore the System:** Restore the system to a normal stage. Restore any data or files that the hacker/cracker may have modified. Install patches or fixes to close any security vulnerabilities that the hacker/cracker may have exploited. Log all actions taken to restore the system to a normal state in a logbook.

d) **Report the Incident:** The incident should be reported following the security incident reporting procedures.

e) **Monitoring:** There are no set procedures for monitoring the activity of a hacker. However, monitored information should be reported in a written log. Each incident will be dealt with on a case-by-case basis. The person authorizing the monitoring activity should provide direction to those doing the monitoring. Once the decision has been made to cease monitoring the hacker's activities and have him removed from the system, the steps outlined previously (i.e., Removal of Hacker/Cracker) are followed.

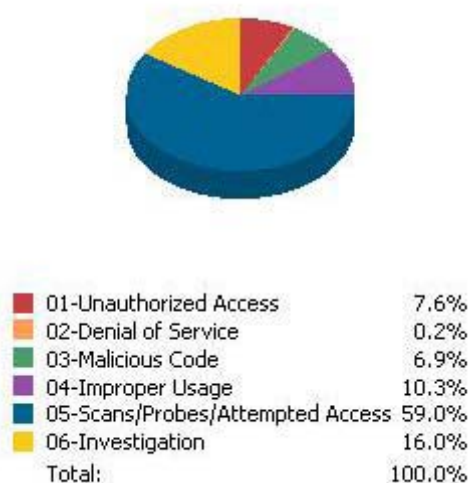


Figure 2 Distribution of Incidents and Responses

The final step of the hacker removal process (i.e., Monitoring) implies an embedded “*If-Then-Else*” statement that requires attention during the modeling phase. Not all hacker activities are alike, and some are considered to be more threatening than others are. Hence a decision is made with every intrusion whether action should be taken or not. To represent this portion of the process, we include a branch that leads to two different organizational responses (i.e., two different task sets), depending upon the threat determination. To help ground this

model in current practice, we draw from the fourth quarter United States Computer Emergency Response Team (US CERT) *Trends and Analysis 2007* (see figure 2 below), which implies that only 16% of hacker/cracker attempts are regarded as minor threats (US CERT, 2007), and hence that the remaining 84% require more extensive organizational responses.

Hierarchy CND Computational Model

Here we describe the Hierarchy CND computational model. Because most CND organizations today reflect like hierarchical structure, this model is representative of the current, prevailing approach to CND. We first outline briefly the specification of this computational model, after which we report simulated performance results for the baseline model. To promote continuity and insight, the discussion here in the main body of the paper is kept purposefully at a relatively high, summary level.

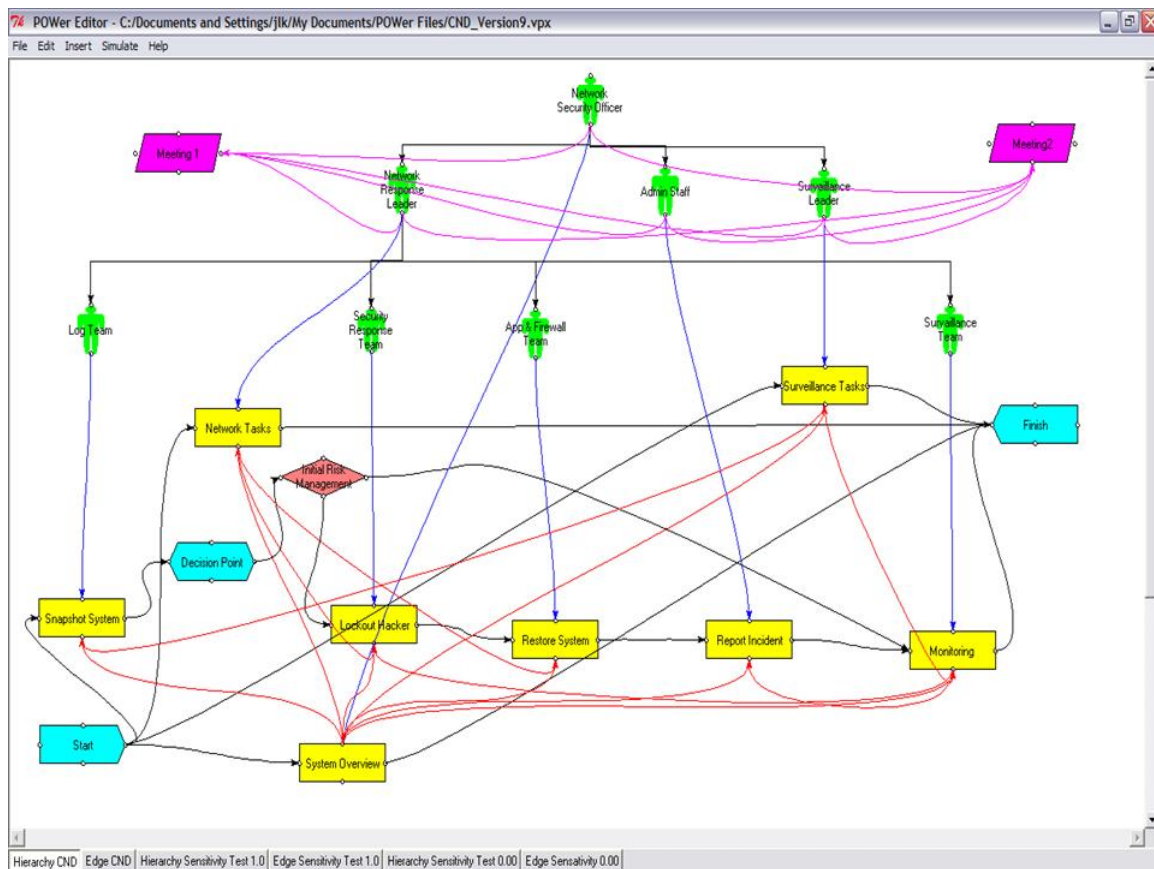


Figure 3 Hierarchy CND Computational Model Screenshot

Figure 3 depicts a POW-ER screenshot for a Hierarchy organization as it responds to a hacker attack. The hacker attack initially observed by the Log Team prompts the middle level managers (Network Response Leader, Administration Staff and Surveillance Leader) and the Network Security Officer to attend a meeting where they assess the threat associated with each specific

hacker attack. If the attack is considered as low threat, and network security is considered adequate for this kind of attack, then the hacker is simply monitored in order to gather information that can be used in legal actions. Alternatively, if the hacker attack is regarded as a serious threat, and network security is deemed to be at stake, the hacker is locked out of the system, and the organization performs a more extensive set of tasks (e.g., Lockout Hacker, Restore System, Report Incident and Monitoring).

Behind each object in the figure one can view a number of model parameters that are set to represent and guide the behavior of the agent-based model. We set most of these parameters at empirically determined “normal” levels, which reflect organizations in general (Jin and Levitt, 1996; Levitt et al., 1999; Nissen and Levitt, 2004). The Hierarchy CND organizational structure is patterned in particular after relevant, previous work (esp. Looney and Nissen, 2006; Gateau et al., 2007). Table 1 summarizes the key model parameterization for this organization and task structure. The reader interested in details is directed to such previous work for elaboration and explanation. This Hierarchy CND model serves as a baseline for comparison of Edge organization.

Parameter	Hierarchical Model Values	Edge Model Values
Centralization	High	Low
Formalization	High	Low
Matrix Strength	Low	High
Team Experience	Low	Medium
Communication Probability	0.10	0.90
Noise Probability	0.30	0.30
Functional Exception Probability	0.10	0.20
Project Exception Probability	0.10	0.20
Rework Strength	0.30	0.10
Meetings	2 hours / day	0
Position Role	ST	SL
Application Experience	Medium	High
Organizational Levels	3	1

Table 1 Summary of Hierarchical and Edge CND Model Parameterization

Edge CND Computational Model

Figure 4 depicts a POW-ER screenshot for the Edge CND organization. The Edge (Alberts and Hayes, 2003) organization provides vivid contrast to the Hierarchy as represented and described above. For direct comparison, the total number of personnel and the total effort level and difficulty of tasks are the same in both models; that is, we control for these important factors, and vary only the organizational form. Notice immediately how the Edge organization lacks the management hierarchy delineated above, as leadership is more emergent in

Edge organizations, and the Edge model is comprised of more, smaller, interdependent teams conducting finer grained sets of tasks. Such tasks are performed more in parallel, and are coordinated more via mutual adjustment (Thompson, 1967), than their Hierarchy counterparts above are. Also, more frequent, lateral communications supplant the meetings prescribed in the Hierarchy model above, and working-level actors collaborate through actions to address each hacker attack. As noted above, most model parameters remain constant across these two organizational forms, and Table 1 above provides details of key parameter settings.

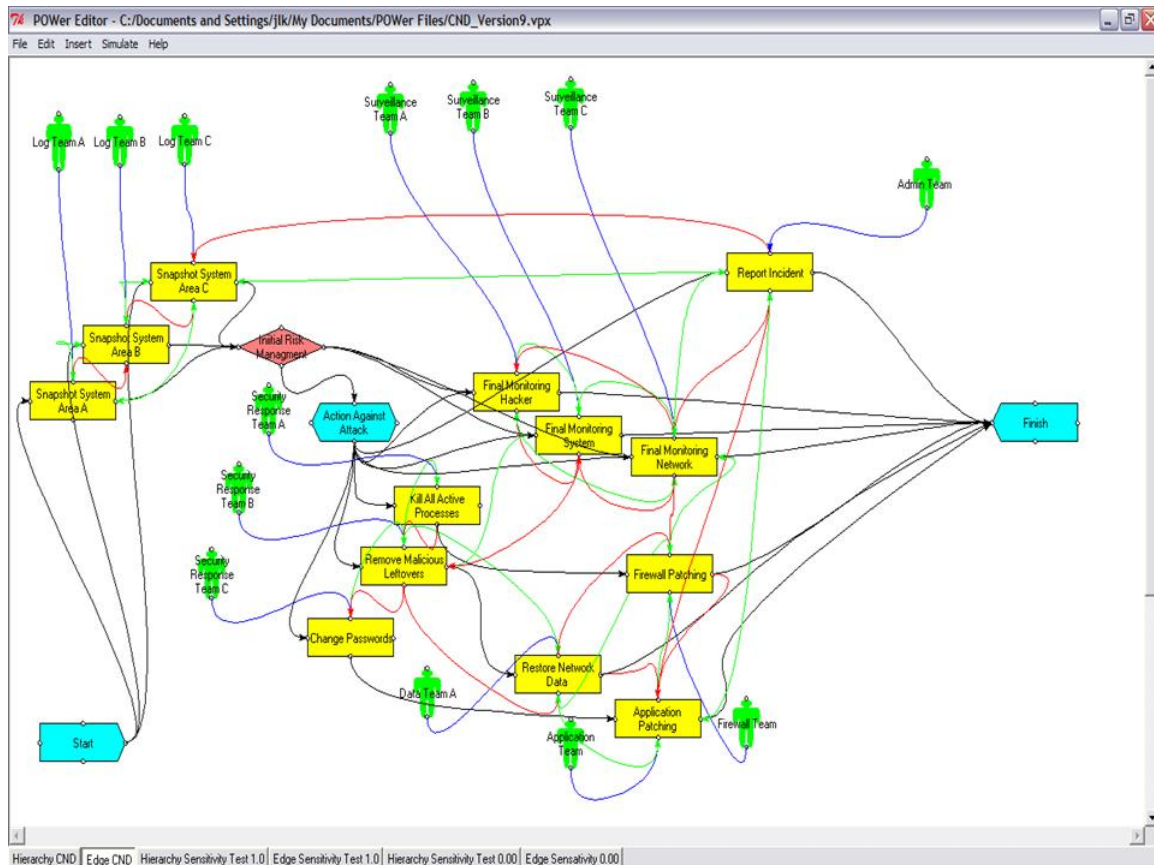


Figure 4 Edge CND Computational Model Screenshot

Experiment Design

In this section we draw from Nissen-Levitt (2004), and build upon Nissen (2005b), to describe briefly the computational methods and tools used for modeling the CND organization and process. The POW-ER agent based modeling application used in this research is version 3.4a, and represents a continuation of development (see Looney & Nissen, 2006; Nissen 2005a; Nissen 2005b). The basic performance and outputs of POW-ER 3.4a have been verified, and several key behavioral and performance results (work duration, functional risk, project risk) have been validated through our fieldwork on the CNO/CND process. Hence we have considerable basis for confidence in the thrust of the

results we report. Additionally, all of the comparisons that we make below are relative to one another, and control for the same underlying variables and behaviors. Hence any bugs or errors inherent in POW-ER 3.4a are controlled and applied consistently across all models. Thus, although one or more of the absolute results reported may be in some error, the relative results reported—which comprise the essence of our study—are reported on a consistent basis.

We take into account current open-source CNO best, and refine the model based upon theoretical inference (Looney & Nissen, 2006; Alberts & Hayes, 2003), drawing heavily upon the previous works in this campaign of Edge. This allows us to model the practical application of modern CNO as it exists today, and to develop Edge-like permutations of this baseline. We then subject the model to a simulated network penetration in both low- and high-threat operational environments. Hence we have a full-factorial, 2 x 3 (i.e., two organizational forms, three mission-environmental contexts), computational experiment, which is consistent with the conduct of previous experiments in this campaign. The interested reader is directed to such prior experiments for details concerning model independent and dependent variables.

More specifically, we examine the performance of each organizational form across three mission-environmental contexts. The first reflects the grounded model input noted above, in which only 16% of hacker attacks are deemed to be serious threats. The low threat model reflects the network being attacked only by “amateur” hackers, and the security deemed to provide adequate protection against them. The only action taken against hacker attacks is continuing to monitor them. Alternatively, the high threat model reflects the network being attacked only by “professional” hackers, and the security deemed to provide inadequate protection against them. The CND organization locks out every hacker. Using a Monte Carlo approach, in which each organization and scenario is run 100 times.

Results

The simulation results are summarized in Table 3 below. We first compare the baseline Hierarchy and Edge results, and then examine their sensitivity to the threat level.

Baseline Comparison

Beginning with the Hierarchy baseline results that are reported in the first row of the table, the CND organization accomplished its network-defense tasks in 5.9 hours; this is a measure of organizational speed, which is very important in the CNO domain. Also, one can see the level of direct work (i.e., planned effort) is 14.2 person-hours; that is, the equivalent of 14 people working for approximately one hour each, or one person working for 14 hours. Rework of 1.3 reflects the level of effort (in person-hours also) expended attending to exceptions and correcting errors that are made during the CND response. Coordination of 3.3 reflects the level of effort (again, in person-hours) expended for coordination between the various CND organizational actors, and 0.2 person-hours of wait time reflect the amount of time that actors spend waiting for decisions to be made

and information to be provided. The 12.0 person-hours spent in meetings should be self-explanatory, as this represents a key approach to coordination in the Hierarchy CND organization. Finally, project risk of 0.2 represents the level of effort (in person-hours) that would be required to attend to all of the exceptions and correcting all of the errors that were either ignored or addressed inadequately.

Table 2 Simulation Performance Results

Scenario	Duration	Direct Work	Rework	Coordination	Wait Time	Meetings	Project Risk
Hierarchy Baseline	5.9	14.2	1.3	3.3	0.2	12.0	0.2
Edge Baseline	5.3	14.6	1.8	4.7	0	0	0.3
Hierarchy Low Threat	5.1	10.0	0.9	3.1	1.4	12.0	0.2
Edge Low Threat	3.5	9.2	0.8	1.4	0	0	0.4
Hierarchy High Threat	5.7	15.0	1.4	3.4	0.2	12.0	0.2
Edge High Threat	5.7	15.2	2.1	5.1	0	0	0.3

For comparison, the Edge requires roughly half an hour less time (5.3 hours) to accomplish its network-defense tasks, and hence moves somewhat more quickly in this mission-environmental context and threat level. This is consistent with results in other contexts (e.g., joint task force, see Gateau et al., 2007; coalition mission planning, see Looney and Nissen, 2006). The Edge also involves slightly more direct work (14.6), due to very small differences in Hierarchy and Edge model representations, but is negligible in the context of this computational experiment. However, it involves a greater level of rework (1.8), which indicates that a greater number of exceptions and errors are made and corrected by the Edge CND organization than the Hierarchy. The Edge organization tends to encounter a greater number of exceptions and make more errors generally than the Hierarchy does. Coordination (4.7) is considerably greater for the Edge, as actors without a hierarchical organization are required to coordinate abundantly and laterally, and Wait Time is zero, as actors in the Edge do not have to wait for supervisors to make decisions or provide information. Notice also that no meetings take place in the Edge; this explains in part the increased coordination load, and reflects the radically different kinds of

organizations, with concomitantly different modes of information processing and behavior, corresponding to the Hierarchy and Edge. Finally, project risk level (0.3) is appreciably higher for the Edge. Hence this organizational form entails greater risk than the Hierarchy does.

To summarize, the Edge CND organization moves more quickly than the Hierarchy does, and it involves zero wait time and meetings. However, the Edge requires a greater level of rework and a considerably greater coordination load, in addition to half again the level of project risk. Hence the CND organization leader and policy maker faces a set of tradeoffs: to the extent that organizational speed is important, the Edge appears to have an edge over the Hierarchy in this context, but to the extent that risk represents a primary concern, the Hierarchy represents the sharper organization. Further, the high coordination load associated with the meetingless and supervisorless Edge organization suggest that this organizational environment may be relatively more stressful for many people—particularly those accustomed to working in formal hierarchies—but the comparative freedom from bureaucracy and direct supervision may be refreshing to many as well. This suggests an opportune area for further research into the organizational climate associated with these alternate forms.

Threat-Level Comparison

In the low-threat environment, both the Hierarchy and Edge move more quickly and involve less effort than in the baseline environment summarized above. Indeed, the Hierarchy reduces its duration (5.1) by nearly a whole hour, and both rework (0.9) and coordination (3.1) are lower. However, notice that the wait time (1.4) is appreciably greater in this low-threat environment. Even though the task environment is comparably simpler than in the baseline context, organizational actors spend considerably more time waiting for supervisors to make decisions and provide information. This represents a drawback of working in even three-level hierarchies: busy supervisors act often as metaphorical bottlenecks, and are central sources of delay.

The Edge moves much more quickly in this low-threat environment than in the baseline, as its duration falls to 3.5 hours. Notice that this represents much greater speed than the Hierarchy (5.1 hours) in this same environment. The Edge also incurs lower levels of both rework (1.4) and coordination (1.4) in this comparatively simple task environment, as task interdependencies are not as demanding as in the baseline, and the flat Edge organizational structure obviates much of the coordination load imposed by the Hierarchy. However, the Edge reflects greater risk (0.4) than in the baseline environment, and even more pronounced than the case described above, the Edge reflects double the risk of the Hierarchy even in this low-threat environment. This may explain in part the lower rework and coordination levels: actors in the Edge organization are failing to attend to exceptions and correct errors to the same extent; hence residual exceptions and errors are reflected in higher risk levels. Here, as above, the CND organization leader and policy maker face similar tradeoffs (e.g., speed vs. risk), but the differences in relative speeds and risk levels are even more pronounced.

By comparison in the high-threat environment, the Hierarchy moves a bit more quickly (5.7 hours) than in the baseline environment summarized above, even though it involves more effort (15.0). Here, 100% of attacks are of the high-threat variety, and this Hierarchy CND organization responds relatively well to them. The other performance parameters differ only negligibly from their baseline counterparts in the Hierarchy.

For the Edge, performance in terms of duration degrades by nearly a half hour (5.7) in this high-threat environment, but is equal to that of the Hierarchy; hence the two organizational forms are equivalent in terms of speed. Rework (2.1) and coordination (5.1) both increase in this environment, and both appear to increase beyond baseline levels by greater margins than reflected in the Hierarchy performance statistics; that is, the Hierarchy appears to be more resilient to a shift to the high-threat environment than the Edge is.

Also as above, the CND organization leader and policy maker face tradeoffs, but the relative speeds are equivalent across both organizational forms, so the lower risk level associated with the Hierarchy makes it appear to be a superior approach in this high-threat environment. Figure 5 illustrates the project risk in all three threat levels.

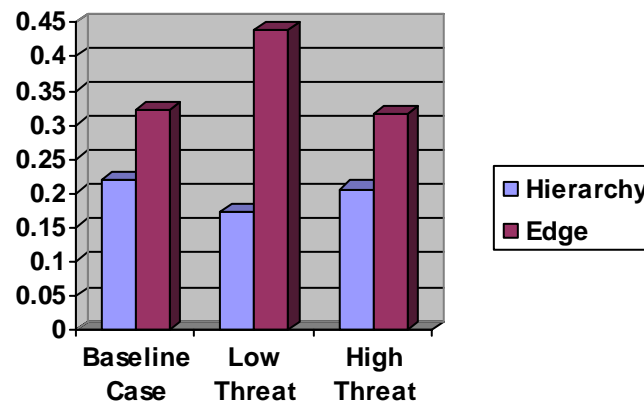


Figure 5 Project Risk

In Figure 6 we present a plot of the project risk and duration values summarized and discussed above. This helps to delineate the key tradeoffs faced by CND organization leaders and policy makers. The horizontal axis represents the duration corresponding to each organization and threat level, and the vertical axis represents the associated risk level. Each organization and threat level point is labeled in the diagram. For instance, the label “HB” corresponds to the Hierarchy organization and baseline threat level that is plotted at the duration (5.9) and risk (0.2) point in the diagram. Likewise, the label “EB” corresponds to the Edge organization and baseline threat level that is plotted at the duration (5.3) and risk (0.3) point in the diagram; “HL” depicts the Hierarchy organization and low threat level; “EL” depicts the Edge organization and low

threat level; “HH” depicts the Hierarchy organization and high threat level; and “EL” depicts the Edge organization and high threat level.

Notice that, as summarized in tabular form above, the Hierarchy exhibits consistently lower risk levels than the Edge does, but aside from the high-threat case, the Edge exhibits consistently lower duration than the Hierarchy does. As noted above, where risk represents the predominate concern, the Hierarchy appears as the clear choice of organizational form. Alternatively, where duration represents the predominate concern, the Edge appears as a marginally better choice in the baseline case, yet this nonhierarchical form represents a considerably superior form in the low-threat case, even though it offers no speed advantage where the threat level is deemed to be high. Hence CND organization leaders and policy makers will need to assess the anticipated threat level associated with a particular mission-environmental context, and they will need to determine, in each such context, whether speed or risk represents the predominate focus in terms of organizational performance.

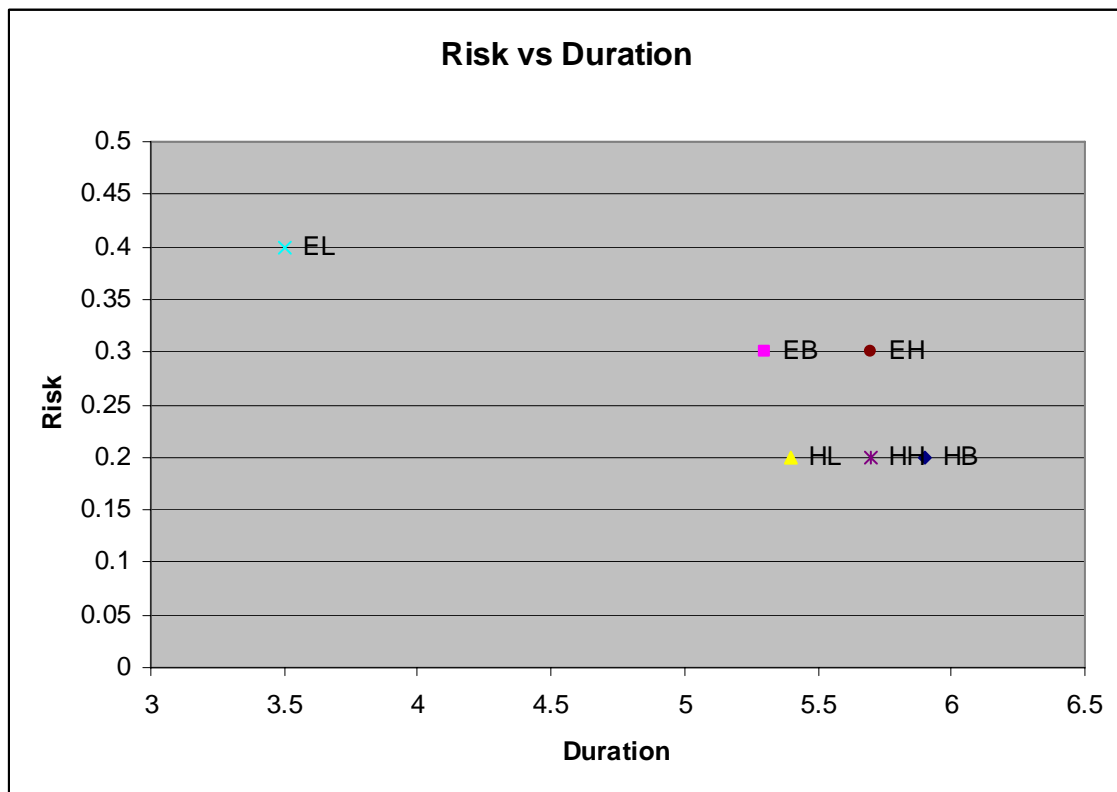


Figure 6 Risk vs. Duration Plot

Consistent with the predictions and empirical support of Contingency Theory, the “best” CND organizational form depends: it depends upon the mission-environmental context, and it depends upon whether speed or risk represents the predominate focus in terms of organizational performance. We summarize these contingent results via the Organizational Fit Matrix presented in Table 3. As noted above, where the threat is low, and leaders and policy makers

deem speed to be the predominate focus, the Edge represents the superior organizational form. Alternatively, where the threat is low, but leaders and policy makers deem risk to be the predominate focus instead, the Hierarchy represents the superior form. Likewise where the threat is high, and leaders and policy makers deem risk to be the predominate focus, the Hierarchy represents the superior form in this case also. An interesting case arises where the threat is high, but leaders and policy makers deem speed to be the predominate focus: here the Hierarchy and Edge reflect equivalent performance in terms of duration, so without specific regard to risk, either form would represent an equivalently superior choice, in a classic case of equifinality.

Table 3 Organizational Fit Matrix

Focus \ Context:	Low Threat	High Threat
Speed	Edge	Either form
Risk	Hierarchy	Hierarchy

Nonetheless, because the Hierarchy matches the speed of the Edge, yet offers lower risk in this high-threat environment, it represents the superior form. Thus, in the CND organizational context, leaders and managers would tend to organize hierarchically unless the threat level is deemed to be relatively, in which case the Edge would represent the superior organizational form. Determining the likely threat levels associated with the myriad, diverse CND organizations in practice represents an obvious follow-on study to the research described in this article. Such study is likely to suggest that, indeed, one size does not fit all: each CND organization should have the latitude to determine its own structure depending upon the focus of leaders and policy makers and the anticipate threat level.

Given what we have observed of Military leaders and policy makers to date, the bias will be clearly toward homogenization of organization; that is, most leaders and policy makers, uncomfortable with the prospect of different organizational forms—despite the benefits in terms of fit and hence performance—will likely take the naïve path, and dictate uniform organization for all, despite the contingent performance degradation associated with such homogenization approach. Further, given that the Hierarchy represents the predominate and familiar organization form in the Military today, the bias will be clearly toward this form—again, despite the benefits in terms of fit and hence performance.

All that we as informed researchers can do is to caution such leaders and policy makers against relenting to their biases, and to encourage them to at least experiment with alternate organizational forms where threat levels are

determined to be low. After all, where threat levels are low, there is little risk in trying a different organizational form, and where the magnitudes and kinds of performance benefits suggested by this study obtain, such leaders and policy makers would be demonstratively short-sighted not to at least try something new, different and hypothetically better. Assessing the comparative performance of alternate CND organizational forms in the field represents an exciting and important subsequent step for this research campaign.

Conclusion

The role of computer networked operations (CNO) has taken on greater importance with the rise of network-centric warfare. Comprised primarily of defense, attack, and exploitation, the technological capabilities are growing exponentially, as is the rate of data exchange, yet the organizational configurations supporting CNO are slow to anticipate and react. This presents a serious issue in terms of command and control (C2), as such organizations do not fit well with their highly dynamic environments, nor are they suited well to the missions and expectations placed upon them. Contingency Theory offers excellent potential to inform leaders and policy makers regarding how to bring their C2 organizations and approaches into better fit, and hence to improve CNO performance. The key research question is, which organizational configurations provide the best CNO performance within the network-centric environment?

Building upon a half century of rich, theoretical and empirical research in Contingency Theory, we construct computational models of CNO set within different organizational configurations taken from both theory and practice, and we employ the method of computational experimentation to examine the comparative performance of such different configurations. Focusing in particular on CND, we develop computational models to represent both the predominate Hierarchy and novel Edge organizational forms, and we examine their relative performance across three different threat levels posed by hackers: 1) a baseline level corresponding to that common in CNO today; 2) a low-threat level associated generally with “amateur” hackers; and 3) a high-threat level associated instead with “professional” hackers. Because these models are developed with the externally validated POW-ER organizational modeling and simulation environment, and because we have grounded our CND models using operational organizations in practice today, we can assert considerable confidence in the empirical results of this investigation.

Results elucidate important insights into CNO C2, suitable for immediate policy and operational implementation. For instance, we reveal how CND leaders and policy makers face tradeoffs between counterbalancing performance interests (esp. speed and risk), and we show how such tradeoffs are sensitive to the threat level associated with any particular CND organization’s mission-environmental context. This results in new knowledge to guide such leaders and policy makers, which we summarize both graphically and tabularly to focus upon the key tradeoffs and correspondingly superior organizational forms. This expands the growing empirical basis to guide continued research along these lines, and it enables leaders and policy makers to move forward immediately,

informed by science supporting the use of different organizational forms in different mission-environmental contexts. We welcome the opportunity to pursue the obvious follow-on research opportunities emanating from this study, and we welcome other researchers to join us in pursuing them.

References

Alberts, D.S. and Hayes, R.E. *Power to the Edge*. Command and Control Research Program, CCRP Publication Series, 2003.

Bryan, James D. Major General, US Army, Commander, Joint Task Force-Computer Network Operations, U.S. Strategic Command and Vice Director, Defense Information Systems Agency. Prepared Statements, before the House Armed Services Subcommittee on Terrorism, Unconventional Threats and Capabilities, Washington, D.C. July 24, 2003.

Burns, T. and Stalker, G. M. *The Management of Innovation*. London: Havistock, 1961.

Burton, R.M., J. Lauridsen, B. Obel. Return on Assets Loss from Situational and Contingency Misfits. *Management Science* 48(11) 1461-1485. 2002.

Carley, K.M., Z. Lin. 1997. A Theoretical Study of Organizational Performance under Information Distortion. *Management Science* 43(7) 976-997.

Ciborra, C. U., "The Platform Organization: Recombining Strategies, Structures, and Surprises," *Organization Science*, vol. 7, pp. 103-118, Mar. - Apr. 1996.

Davidow, W. H. and Malone, M. S. *The Virtual Corporation*. New York, NY: Harper Business, 1992.

Department of Defense, 2006. Information Operations Roadmap (classified document dated 2003). Washington.
<http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/>

Donaldson, Lex. *The Contingency Theory of Organizations*, Thousand Oaks, Sage Publications, 2001.

Franz. T. Et al. 2007. Defining Information Operations Forces: What Do We Need? *Air and Space Journal* Summer 2007.
<http://www.airpower.maxwell.af.mil/airchronicles/apj/apj07/sum07/franz.html>

Galbraith, J. R., *Designing Complex Organizations*. Boston, MA: Addison-Wesley Longman Publishing Co., Inc, 1973.

Galbraith, J.R. *Organizational Design*. Addison-Wesley, 1977.

Gateau, J.B. Et al. Hypothesis Testing of Edge Organizations: Modeling the C2 Organization Design Space. *Proceedings International Command and Control Research and Technology Symposium*, Newport, Rhode Island. June 2007.

Harvey, E., "Technology and the Structure of Organizations," *American Sociology Review.*, vol. 33, pp. 247- 259, April. 1968.

Jin, Y., R.E. Levitt. 1996. The Virtual Design Team: A Computational Model of Project Organizations. *Journal of Computational and Mathematical Organizational Theory* 2(3) 171-195.

Joint Chiefs of Staff, 2006. Joint Publication 1-02: Dictionary of Military Terms. http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf

Joint Chiefs of Staff, 2006. Joint Publication 3-13: Information Operations. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf

Lawrence, P.R., and Lorsch, J.W. 1967. Differentiation and Integration in Complex Organizations. *Administrative Science Quarterly*, 12, 1-47.

Lawrence, P.R. and Lorsch, J. W. *Organization and Environment: Managing Differentiation and Integration*. Boston, MA: Division of Research, Harvard Business School Press, 1967.

Levitt, R.E., J. Thomsen, T.R. Christiansen, J.C. Kunz, Y. Jin, C. Nass. 1999. Simulating Project Work Processes and Organizations: Toward a Micro-Contingency Theory of Organizational Design. *Management Science* 45(11):1479-1495.

Leweling, T.A. and Nissen, M.E., "Hypothesis Testing of Edge Organizations: Laboratory Experimentation using the ELICIT Multiplayer Intelligence Game," *Proceedings International Command & Control Research & Technology Symposium*, Newport, RI, June 2007.

Lomi, A., E.R. Larsen. *Dynamics of Organizations: Computational Modeling and Organization Theories*, Menlo Park, CA, American Association of Artificial Intelligence, 2001.

Looney, J.P. and Nissen, M.E., "Computational Modeling and Analysis of Networked Organizational Planning in a Coalition Maritime Strike Environment," *Proceedings Command & Control Research & Technology Symposium*, San Diego, CA, June 2006.

Miles, R. E. and Snow, C. C. *Organizational Strategy, Structure, and Process*. New York, NY: McGraw-Hill, 1978.

Mintzberg, Henry. *The Structuring of Organizations* Englewood Cliffs, NJ: Prentice-Hall, 1979.

- Mintzberg, Henry. 1980. Structure in 5's" A Synthesis of the Research on Organization Design. *Management Science*. Mar; 26(3):322-341.
- Mohr, L. B., "Organizational Technology and Organizational Structure," *Administrative Science Quarterly*, vol. 16, pp. 444-459, December. 1971.
- NAACSOS. 2007. North American Computational Social and Organization Sciences, website <http://www.casos.cs.cmu.edu/naacsos/>, accessed 13 March 2007.
- Nissen, M.E. 2005a. Hypothesis Testing of Edge Organizations: Specifying Computational C2 Models for Experimentation. *Proceedings International Command & Control Research Symposium*. McLean, VA, June 2005.
- Nissen, M.E., 2005b. "A Computational Approach to Diagnosing Misfits, Inducing Requirements, and Delineating Transformations for Edge Organizations," *Proceedings International Command and Control Research and Technology Symposium*, McLean, VA , June 2005.
- Nissen, M.E. and Buettner, R.R. "Computational Experimentation with the Virtual Design Team: Bridging the Chasm between Laboratory and Field Research in C2," *Proceedings Command and Control Research and Technology Symposium*, San Diego, CA, June 2004.
- Nissen, M.E., R.E. Levitt. 2004. Agent-Based Modeling of Knowledge Dynamics. *Knowledge Management Research & Practice* 2(3) 169-183.
- Orr, R.J. and Nissen, M.E., "Computational Experimentation on C2 Models," *Proceedings International Command and Control Research and Technology Symposium*, Cambridge, UK, September 2006.
- Ouchi, W. G. *Theory Z: How American Business can Meet the Japanese Challenge*. Reading, MA: Addison-Wesley, 1981.
- Pennings, J. M., "The Relevance of the Structural-Contingency Model for Organizational Effectiveness," *Administrative Science Quarterly*, vol. 20, pp. 393-410, September. 1975.
- Perrow, C. *Organizational Analysis: A Sociological View*. Belmont, CA: Wadsworth, 1970.
- Scott, W.R. *Institutions and Organizations* (Second Edition) Thousand Oaks, CA: Sage, 2001.
- Simon, H. A. *The Sciences of the Artificial* (3rd ed.), Cambridge, MA, the MIT Press, 1996.

Thompson, J.D. *Organizations in Action*, New York, McGraw-Hill, 1967.

UCSF IT Network Architecture & Security: Security: Incident Response.

Retrieved 3/18/2008, 2008, from

http://itnas.ucsfmedicalcenter.org/security/incident_response/

United States Army Training and Doctrine Command, 2005. Cyber Operations and Cyber Terrorism; handbook no. 1.02. Fort Leavenworth, KS.

<http://www.au.af.mil/au/awc/awcgate/army/guidterr/sup2.pdf>

US-CERT: United States Computer Emergency Readiness Team. Retrieved 3/18/2008, 2008, from <http://www.us-cert.gov/>

Vega, J. *Computer Network Operations Methodology*. Master's Thesis, Naval Postgraduate School, Monterey, CA, 2004.

Whitehouse, 1998. Presidential Decision Directive 63: Critical Infrastructure Protection. Washington. <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>

Wilson, C. 2007. Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues. Washington: CRS, 2007.

<http://www.fas.org/sgp/crs/natsec/RL31787.pdf>

Woodward, J. *Industrial Organization: Theory and Practice*. New York, NY: Oxford University Press, 1965.



C2 for Computer Networked Operations: Using Computational Experimentation

Major Jack L. Koons III
Lieutenant JG Nikolaos Bekatoros,
Dr. Mark E. Nissen
US Naval Postgraduate School

Motivation

- Rise of NCW & CNO
- Highly Dynamic Environments
- Asymmetric Threats
- DoD Grappling with C2 and Organization Issues
- Contingency Theory and Computational Modeling
- *Which Organizations Provide the Best CNO Performance within the NWC Environment?*

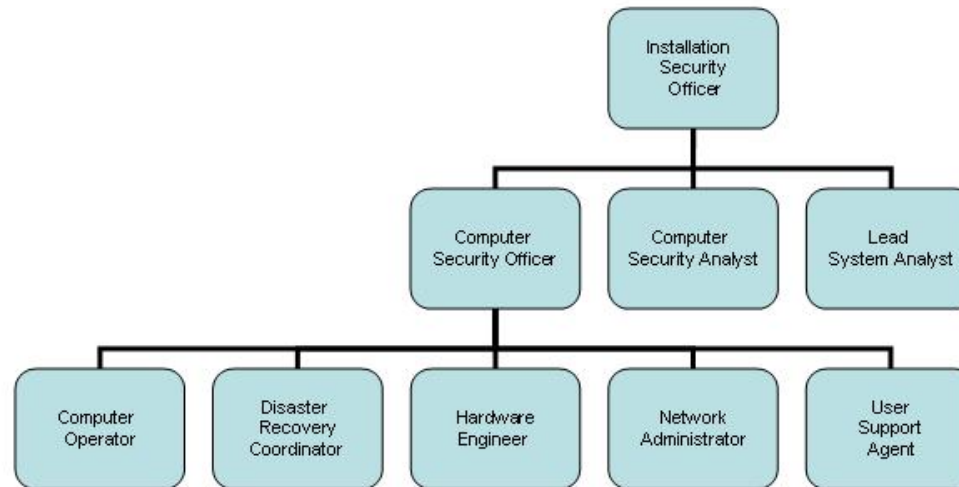
Prior Research

- Center for Edge POW-ER at NPS
 - Contingency Theory
 - Computational Modeling
- Campaign of Experimentation
 - Buettner & Nissen 2004
 - Nissen 2005
 - Orr & Nissen 2006
 - Gateau, Looney, Leweling & Nissen 2007

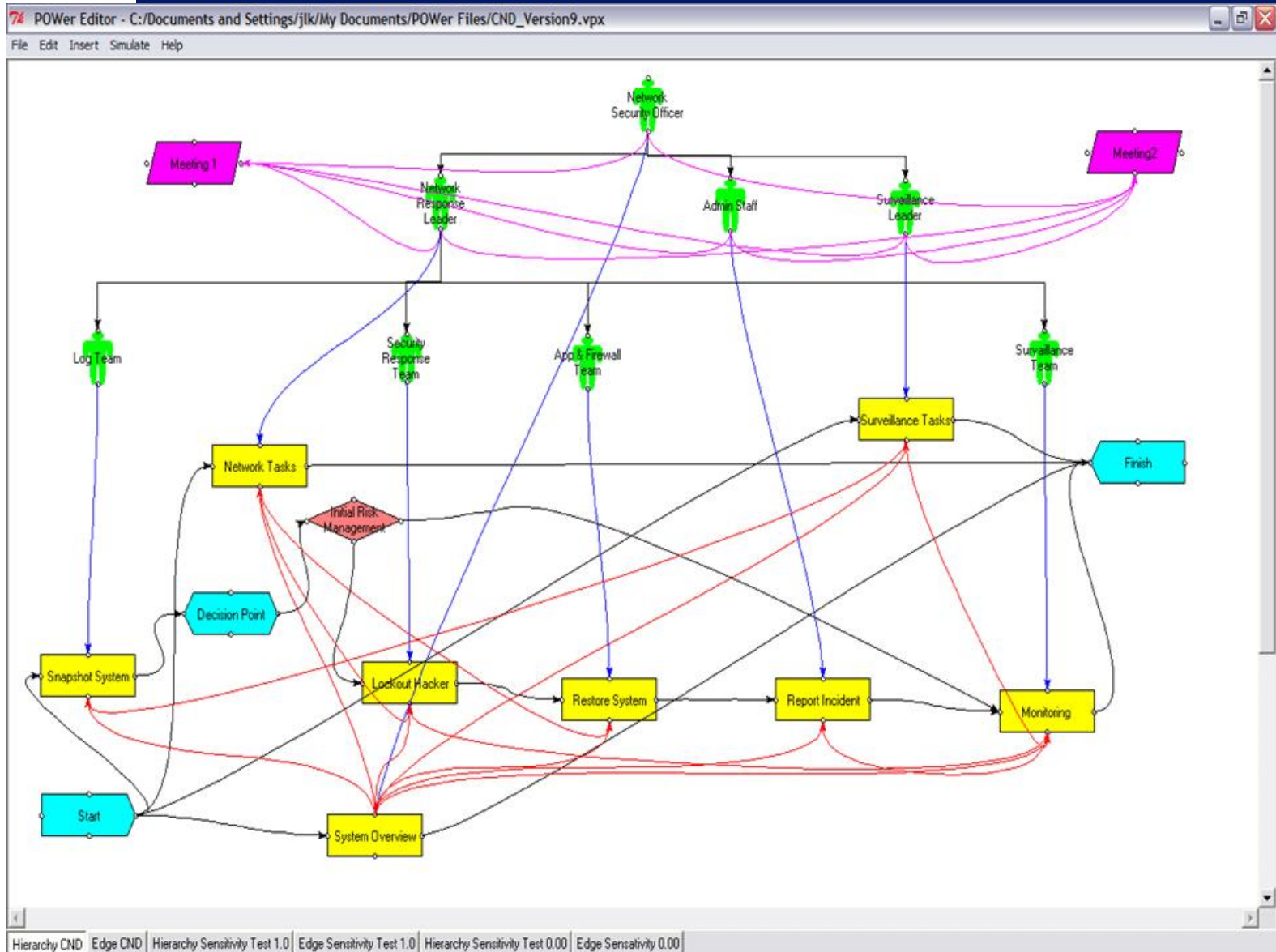
Grounded CNO Model

- CNO
 - Attack (CNA)
 - Exploit (CNE)
 - Defend (CND) *This is our focus!*
- Generalized Model
 - Similar Approach by Military and Industry
 - ◇University of California San Francisco Medical Center
 - ◇NPS Information Technology
 - ◇Subject Matter Experts

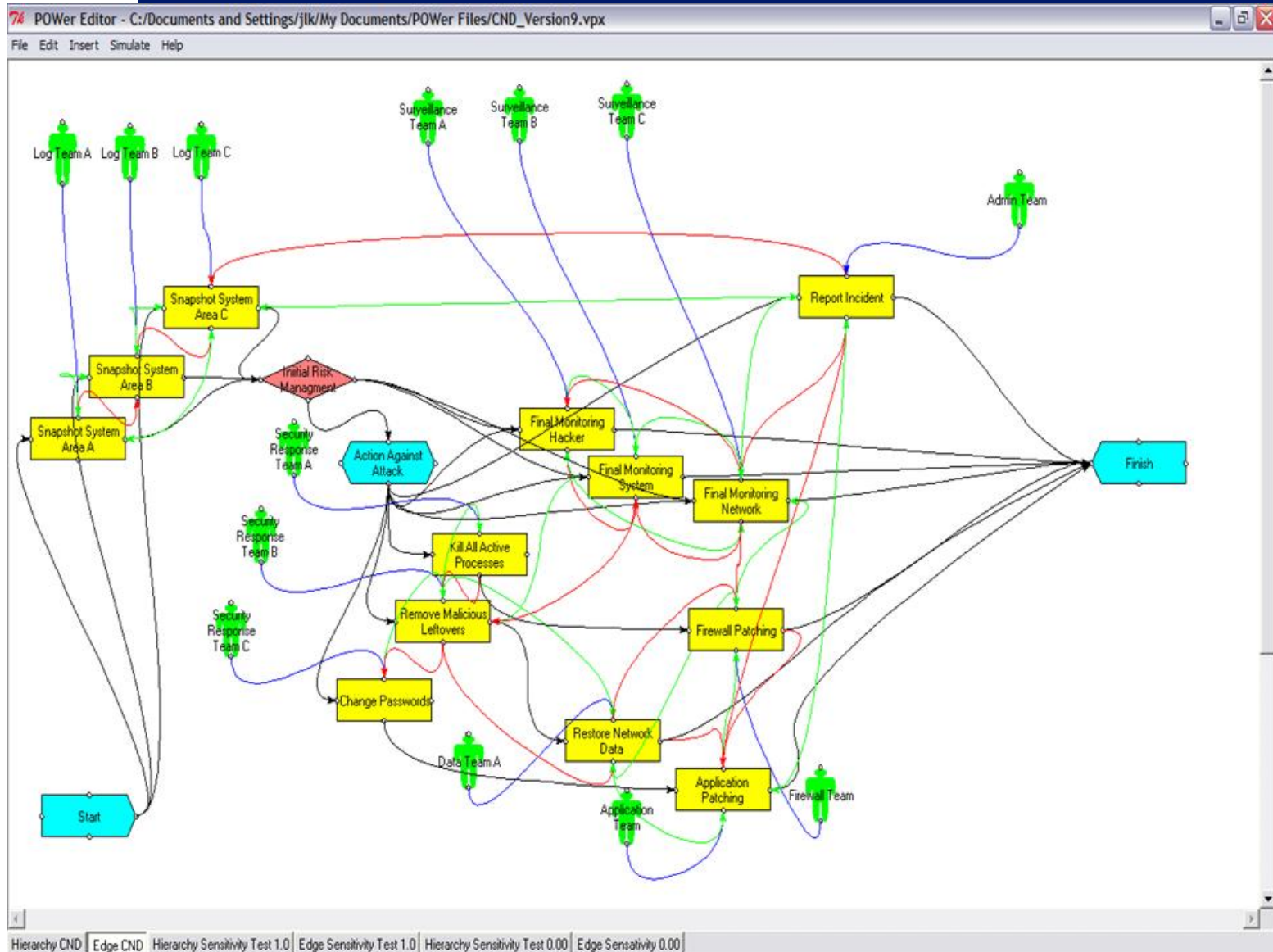
Grounded CND Organization



Hierarchy POW-ER Model



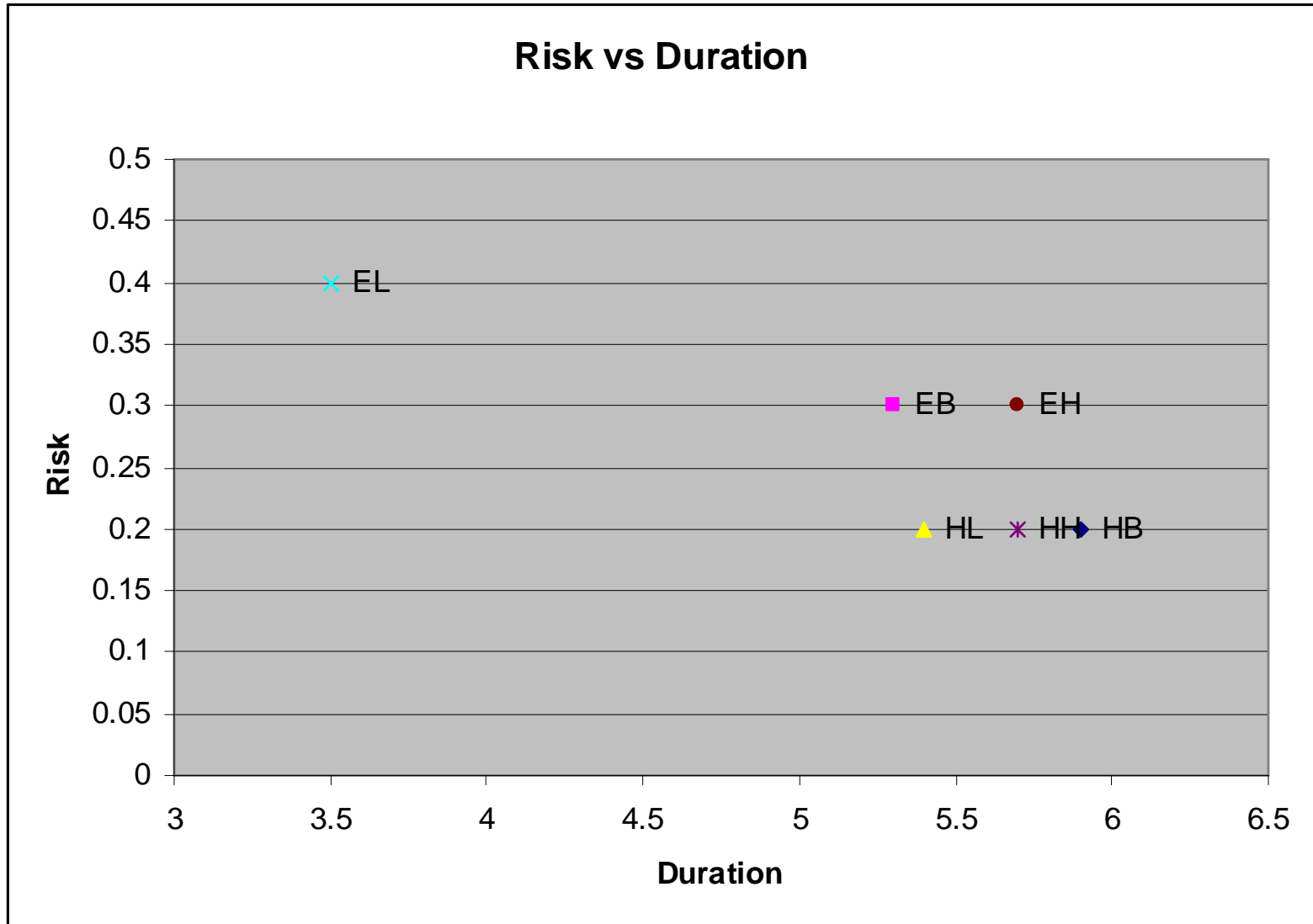
Edge POW-ER Model



Simulated Performance

Scenario	Duration	Direct Work	Rework	Coordination	Wait Time	Meetings	Project Risk
Hierarchy Baseline	5.9	14.2	1.3	3.3	0.2	12.0	0.2
Edge Baseline	5.3	14.6	1.8	4.7	0	0	0.3
Hierarchy Low Threat	5.1	10.0	0.9	3.1	1.4	12.0	0.2
Edge Low Threat	3.5	9.2	0.8	1.4	0	0	0.4
Hierarchy High Threat	5.7	15.0	1.4	3.4	0.2	12.0	0.2
Edge High Threat	5.7	15.2	2.1	5.1	0	0	0.3

Risk vs. Duration Plot



Organizational Fit Matrix

Focus	\	Context:	Low Threat	High Threat
Speed			Edge	Either form
Risk			Hierarchy	Hierarchy

Contributions

- Which Organizations Provide the Best CNO Performance within the NWC Environment?
- Predominate Hierarchy vs. Novel Edge CND
- Balance Trade-offs
 - Risk
 - Speed
 - Threat Level Sensitivity

Limitations and Future Research

- Computational Modeling Vice “Real World”
- Validation in “Live” CNO Environment
- Organizational Consultant (OrgCon)
 - Fit and Misfit
 - Operational Environment

Questions and Comments

